RECEIVED
CENTRAL FAX CENTER
SEP 0 1 2006

REMARKS

This response is intended as a full and complete response to the final Office Action mailed July 25, 2006. In the Office Action, the Examiner notes that claims 1-9 are pending and rejected.

In view of the following discussion, Applicant submits that none of the claims now pending in the application are obvious under the provisions of 35 U.S.C. §103. Thus, Applicant believes that all of these claims are now in allowable form.

It is to be understood that Applicant does not acquiesce to the Examiner's characterizations of the art of record or to Applicant's subject matter recited in the pending claims. Further, Applicant is not acquiescing to the Examiner's statements as to the applicability of the art of record to the pending claims by filing the instant response.

35 U.S.C. §103 Rejection of Claims 1-6, 8-9

Claims 1-6 and 8-9 are rejected under 35 U.S. C. §103(a) as being unpatentable over U.S. Patent Application Publication Number 2002/0031134 to Poletto et al. (hereinafter Poletto) in view of U.S. Patent Application Publication No. 2002/0035698 to Malan et al. (hereinafter Malan). Applicant respectfully traverses the rejection.

Poletto discloses a system architecture for thwarting denial of service attacks on a victim data center. The system includes monitors which monitor network traffic flow through the network, and a central controller that receives data from the plurality of monitors. The central controller analyzes network traffic statistics to identify malicious network traffic. (Poletto, Abstract).

Poletto, however, fails to teach or suggest each and every element of Applicant's invention. Namely, as admitted by the Examiner, Poletto fails to teach or suggest at least the limitations of "controlling a network switch to divert a predetermined fraction of SYN packets destined for said server, to a web guard processor" and "monitoring the number of timed-out connections between said web guard processor and said one or more clients, and, if the number of timed-

out connections between said web guard processor and said one or more clients exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor," as taught in Applicant's invention of at least claim 1.

Furthermore, Malan fails to bridge the substantial gap as between Poletto and Applicant's invention.

Malan discloses a method and system for protecting publicly accessible network computer services from undesirable network traffic. Network traffic destined for the network computer services is received and analyzed in order to identify an undesirable user of the services. As disclosed in Malan, topologically anomalous application-level patterns of traffic are identified and removed from the network. (Malan Abstract). As further disclosed in Malan, network topology information and coarse-grained traffic statistics from routers are used to detect, backtrack, and filter network attacks.

Malan, however, is devoid of any teaching or suggestion of diverting a predetermined fraction of SYN packets destined for a server to a processor. Furthermore, Malan is devoid of any teaching or suggestion of controlling a switch to divert all SYN packets intended for a server to a processor if the number of timed-out connections between the processor and one or more clients exceeds a predetermined threshold. Rather, Malan merely teaches a suite of data mining, network profiling, event correlation and monitoring protocols and techniques for detecting denial of service attacks, tracing the source of the attack, and blocking the attacks as close to the source as possible. As such, Malan, alone or in combination with Poletto, fails to teach or suggest Applicant's invention, as a whole.

Furthermore, in the Office Action, the Examiner cites a specific portion of Malan for teaching Applicant's limitations of "controlling a network switch to divert a predetermined fraction of SYN packets destined for said server, to a web guard processor" and "monitoring the number of timed-out connections between said web guard processor and said one or more clients, and, if the number of timed-out connections between said web guard processor and said one or more clients

exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor," as taught in Applicant's invention of at least claim 1. The cited portions of Malan, however, merely recite:

> "[0108] FIG. 10 demonstrates the utility of the StormDetector system. A host in ISP-A is bombarding a target server in the Web hosting service with a denial of service attack. However, the attacker is forging the return address on the packets in the attack, making is impossible to determine their true origin. The StormDetector's analysis engine receives flow statistics from the routers in the target's hosting service. From these statistics, it can detect the attack at some-set of the affected routers along its path. This path leads directly from the target to ISP-A's border, where the attack originates. This example demonstrates the utility of the StormDetector deployed within a Web hosting service's network. It can also be used in both source and transit networks.
>
> [0109] When employed at an attacker's originating network, StormDetector can pinpoint the location of the attacker. In this case, it will backtrack the attack directly to its source's first-hop router. It may be that the attacker is a zombie residing on a compromised machine in an enterprise network. In addition to uncovering those traditional launchpads, StormDetector will be instrumental in identifying attacks originating from home machines that connect to the Internet through persistent tier-2 ISP's ADSL or cable modem connections.
>
> [0110] FIG. 9 represents the process for detecting anomalies in the network statistics within a single zone. At the start, the system picks a measurement node at random. A set of coarse flow statistics or packet header samples is collected. This set of statistics is examined for anomalies. These anomalies include both clearly defined misuse of the network resources, and also significant differences between the profile of the various endpoints and the behavior measured in the sample. If any new anomalies are detected in the sample, they are added as conditional anomalies, and the collector is updated with these new conditional anomalies. Next, a refined sample is taken with respect to the pending conditional anomalies at the collector. The system then looks at the refined sample of the network statistics for the presence of both new conditional anomalies as well as old anomalies. For each anomaly found, its status is updated. The system then goes through the outstanding anomalies and prunes out any stale ones.

> Finally, the system updates the database with the latest summary statistics for each of the outstanding anomalies. The system then repeats, by beginning at the start node."
> [Malan, Para. 0108 – 0110].

The cited portion of Malan is entirely different than the claimed invention. The cited portion of Malan merely describes a StormDetector system that receives flow statistics from routers in the target's hosting service, and from the statistics, detects the attack at some set of the affected routers along a path from the target of the attack to the border of the ISP where the attack originates. The StormDetector system pinpoints the location of the attacker by backtracking the attack directly to its source's first-hop router. The cited portion of Malan further describes a process for analyzing collected statistics in order to detect anomalies in the collected statistics.

As such, the cited portion of Malan is completely devoid of any teaching or suggestion of diverting any traffic from a server to a processor. Furthermore, the cited portion of Malan is completely devoid of any teaching or suggestion of any connections between clients and a web guard processor and between the web guard processor and a server, much less timed-out connections, monitoring the number of timed-out connections, or taking any action in response to the number of timed-out connections exceeding a threshold. Moreover, even if Malan did teach monitoring for such timed-out connections and taking action in response to the number of timed-out connections between clients and processor (which Malan clearly does not), Malan still fails to teach or even suggest diverting all SYN packets destined to the server to the web guard processor, as taught in Applicant's claim 1. As such, Malan, alone or in combination with Poletto, fails to teach or suggest Applicant's invention of at least claim 1, as a whole.

The test under 35 U.S.C. §103 is not whether an improvement or a use set forth in a patent would have been obvious or non-obvious; rather the test is whether the claimed invention, considered as a whole, would have been obvious. Jones v. Hardy, 110 USPQ 1021, 1024 (Fed. Cir. 1984) (emphasis added). Moreover, the invention as a whole is not restricted to the specific subject matter claimed, but also embraces its properties and the problem it solves. In re Wright,

6 USPQ 2d 1959, 1961 (Fed. Cir. 1988) (emphasis added). Poletto and Malan, alone or in combination, fail to teach or suggest Applicant's invention as a whole.

As such, Applicant submits that independent claim 1 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, independent claim 8 recites limitations similar to the limitations of claim 1. Thus, for at least the same reasons discussed herein with respect to claim 1, Applicant submits that independent claim 8 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

As such, Applicant submits that independent claims 1 and 8 are not obvious and fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder. Furthermore, claims 2-6 and 9 depend directly or indirectly from independent claims 1 and 8 and inherit the patentable subject matter of independent claims 1 and 8, while reciting additional elements. For at these the same reasons discussed above, these dependent claims also are not obvious and fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Accordingly, Applicant respectfully requests that the rejection against the claims be withdrawn.

35 U.S.C. §103 Rejection of Claims 7

Claim is rejected under 35 U.S. C. §103(a) as being unpatentable over U.S. Patent Application Publication Number 2002/0031134 to Poletto et al. (hereinafter Poletto) in view of U.S. Patent Application Publication No. 2002/0035698 to Malan et al. (hereinafter Malan). Applicant notes, however, that only Poletto is applied against claim 7. Applicant respectfully traverses the rejection.

As described herein, Poletto discloses a system architecture for thwarting denial of service attacks on a victim data center. The system includes monitors which monitor network traffic flow through the network, and a central controller that receives data from the plurality of monitors. The central controller analyzes network traffic statistics to identify malicious network traffic. (Poletto, Abstract).

Poletto, however, fails to teach or suggest any of the elements of Applicant's invention of claim 7. Applicants' claim 7 recites:

> "A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server disposed in a network of interconnected elements communicating using the TCP protocol, the attack originating from a host generating SYN packets destined for the server, said method comprising:
> arranging a switch receiving the SYN packets destined to the server to forward the SYN packets to a TCP proxy arranged to operate without an associated cache,
> for each SYN packet, sending a SYN/ACK packet from the TCP proxy to a sender address included in the SYN packet by the host;
> establishing a TCP connection, corresponding to a particular SYN packet of the SYN packets, between the TCP proxy and the server only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet."

As such, Applicant's invention discloses that a switch receiving SYN packets from a client intended for a server is arranged to forward the SYN packets to a TCP proxy arranged to operate without an associated cache. For each SYN packet received by the TCP proxy, the TCP proxy sends a SYN/ACK packet to the sender address included in the SYN packet. Then, if the TCP proxy receives a response from the host to the SYN/ACK packet, the TCP proxy establishes a TCP connection between the TCP proxy and the server for which the SYN packet was intended. As such, as taught in Applicant's invention, the server is isolated from the TCP handshake process by the TCP proxy. The TCP proxy of Applicant's invention verifies the TCP handshake before the TCP proxy completes the connection between the host and the server by establishing a TCP connection between the TCP proxy and server.

By contrast, Poletto teaches a gateway disposed between a client and a server. The gateway receives a SYN packet from the client and forwards the SYN packet to the server. In other words, as taught in Poletto, the gateway forwards the SYN packet to the server for which the packet is intended, not to a TCP proxy, as taught in Applicant's claim 1. As such, Poletto does not teach Applicant's limitation of arranging a switch receiving the SYN packets destined to

the server to forward the SYN packets to a TCP proxy arranged to operate without an associated cache, as taught in Applicant's claim 7.

In further contrast to Applicant's invention, Poletto teaches that the server generates the SYN/ACK packet in response to the SYN packet, and sends the SYN/ACK packet to the gateway, which forwards the SYN/ACK packet to the associated client. In other words, as taught in Poletto, the server for which the SYN packet was intended sends the associated SYN/ACK packet to the client. Although the SYN/ACK packet in the Poletto system traverses the gateway in the path between the server the client, the SYN/ACK packet is not sent from the gateway. Furthermore, as described herein, the gateway is simply not a TCP proxy. As such, Poletto does not teach Applicant's limitation that the SYN/ACK packet is sent from a TCP proxy to the sender address included in the SYN packet by the host, as taught in Applicant's claim 7.

In further contrast to Applicant's invention, Poletto teaches that the gateway immediately sends an ACK packet to the server to close the three-way handshake. By contrast, since, as taught in Applicants' invention, the TCP proxy sends a SYN/ACK packet back to the host in response to the SYN packet, Applicant's invention teaches that the TCP proxy waits until it receives, from the host, a response to the SYN/ACK packet. The transmission of an ACK packet from a gateway to a server in response to a SYN/ACK packet received by the gateway from the server, as taught in Poletto, is not transmission of a response from the client to the TCP proxy in response to a SYN/ACK packet received by the client from the TCP proxy, as taught in Applicant's claim 7.

Furthermore, as taught in Applicant's invention, if the TCP proxy receives, from the host, a response to the SYN/ACK packet, the TCP proxy completes the connection between the host and the server by establishing a TCP connection between the TCP proxy and the server. There is no teaching or suggestion in Poletto that the gateway establishes a TCP connection to the server. This is simply not required in the Poletto system since there is already a TCP connection between the client and the server which is used in the TCP handshake process. As such, Poletto fails to teach or suggest Applicant's limitation of "establishing a

TCP connection, corresponding to a particular SYN packet of the SYN packets, between the TCP proxy and the server only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet," as taught in Applicant's claim 7.

Moreover, Applicant respectfully submits that Malan, alone or in combination with Poletto, fails to teach or suggest Applicants' invention of at least claim 7, as a whole.

As such, Applicant submits that independent claim 7 is not anticipated in view of Poletto, or obvious in view of Poletto and Malan, and fully satisfies the requirements of 35 U.S.C. §§102, 103 and is patentable thereunder.

Accordingly, Applicant respectfully requests that the rejection against the claims be withdrawn.

CONCLUSION

Thus, Applicant submits that claims 1-9 are in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, it is requested that the Examiner telephone Michael Bentley or Eamon J. Wall at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

8/31/06

Eamon J. Wall, Attorney
Reg. No. 39,414
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Suite 100
Shrewsbury, New Jersey 07702